UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
THE SUBJECT DEVICE, IDENTIFIED IN ATTACHMENT A

Case No. 3:20-MJ-506
Magistrate Judge Michael J. Newman

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
See attachment A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:
See attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. §§ 841(a)(1), (b)(1)(B) and (b)(1)(C)	Possession of a controlled substance.
18 U.S.C. § 922(g)(1)	Possession of a firearm by a prohibited person.

The application is based on these facts:
See affidavit of SA Christopher Reed

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

CHRISTOPHER REED
Digitally signed by CHRISTOPHER REED
Date: 2020.10.23 14:02:02 -04'00'
Applicant's signature

SA Christopher Reed, ATF
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by _____ *(specify reliable electronic means).*

Date: **3:19 PM, Oct 23, 2020**

City and state: **Via electronic means.**

Michael Newman

Michael J. Newman
United States Magistrate Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF THE SIBJECT DEVICE, IDENTIFIED IN ATTACHMENT A	Case No. 3:20-MJ-506

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Christopher Reed, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device more fully described in Attachment A—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), and have been so employed since May of 2008. Prior to my employment with ATF, I received additional law enforcement training at the Indianapolis Police Department's Police Academy. I was a sworn police officer with the Indianapolis Metropolitan Police Department (IMPD) for approximately (8) years. As a police officer, I conducted investigations in the duty capacity as a uniform officer, narcotics detective and as an ATF Task Force Officer. I have been involved in numerous investigations of federal firearms and controlled substances

violations. These investigations have resulted in the arrest and conviction of criminal defendants. Through my training and experience, I know that drug traffickers oftentimes possess distribution amounts of controlled substances, proceeds of drug trafficking, and firearms to protect both their proceeds and controlled substances. Drug traffickers often utilize cellular devices to communicate with sources of supply and customers to further their operations.

3. This affidavit is submitted in support of an application for a federal search warrant for the following device as there is probable cause to believe that evidence of a crime-namely, Possession with Intent to Distribute a controlled substance in violations of 21 U.S.C. §§ 841(a)(1) (b)(1)(B) and (b)(1)(C), and 18 U.S.C. §§ 922(g)(1)/ 924(a)(2) namely; Possession of a Firearm by a Prohibited Person.

4. On or about June 2, 2020, Luis GARZA (hereinafter referred to as "GARZA") was indicted by a federal grand jury for firearm and controlled substance violations in relation to this investigation. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is more fully described in Attachment A but is described at follows:

- BLUE SAMSUNG GALAXY S9+ SMARTPHONE, with IMEI: 357930090160505

hereinafter the "DEVICE." The DEVICE is currently located in the custody of the Springfield Police Division, Springfield, Ohio.

6. The applied-for warrant would authorize the forensic examination of the DEVICE for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. On or about October 24, 2019, Springfield Police Division (SPD) Investigators received a phone call from Ohio Adult Parole Officer Beatty in reference to GARZA, a parolee of his, who was on parole for Aggravated Robbery and the subject of a traffic stop in Indiana. Parole Officer Beatty requested the assistance of SPD with conducting a parole search of GARZA's listed residence of 1606 Kenwood Avenue, Springfield, Ohio while GARZA was detained in Indiana.

8. Upon arriving at the location, Ohio Adult Parole and law enforcement made contact with the residence occupant, Mallory SHAWVER. During conversation, Ms. SHAWVER advised the Parole Officers there was a firearm inside the residence and provided them with the firearm's location. During the execution of the parole search, a black scale and suspected controlled substances were located on the premises. Ms. SHAWVER signed a SPD Consent to Search form for the 1606 Kenwood Avenue location as law enforcement continued their search. An assortment of items, which included suspected controlled substances, United States currency, along with a firearm and ammunition were recovered from the location by the conclusion of their search.

9. The suspected controlled substances were later submitted to the Bureau of Criminal Investigation (BCI) Laboratory for analysis. The BCI Laboratory Analysis report identified the substances contained approximately 14 grams of Carfentanil, a Schedule II

controlled substance, approximately 28 grams of Fentanyl, a Schedule II controlled substance, and approximately 114 grams of Methamphetamine, a Schedule II controlled substance.

10. On or about October 25, 2019, SPD Investigators conducted an interview of GARZA at the Henry County Sheriff Office located in Henry County, Indiana. At the beginning of the interview, GARZA was provided his Miranda warnings, that were read to him from a Henry County Sheriff Advice of Rights form. GARZA indicated that he understood his rights, signed the form and agreed to speak with the SPD investigator.

11. During the course of the interview, the SPD investigator told GARZA that parole had conducted a search of his residence the previous day. GARZA acknowledged the 1606 Kenwood Avenue location as his residence and that he currently lived there with his child's mother, Mallory. The SPD investigator told GARZA that a firearm, along with suspected controlled substances were located at the residence during the search. GARZA claimed ownership of the firearm and controlled substances located by investigators.

12. Prior to leaving the Sheriff Office, the SPD investigators were provided with the DEVICE, which was found in GARZA's possession at the time of his arrest in Indiana. The DEVICE is currently in the lawful possession of the Springfield Police Division, located in Springfield, Ohio.

13. Because of the drugs found at the defendant's residence, on October 28, 2019, officers with Henry County, Indiana Sheriff's Office went to the secure tow yard where GARZA's vehicle was impounded on a police hold. Officers ran a canine around the vehicle and the canine alerted. Officers obtained a state search warrant to search the vehicle. Officers located

two vacuum sealed packages containing a white crystal substance in a compartment between the rear seats. The substance was analyzed by the Drug Enforcement Administration laboratory and was found to contain approximately 892.4 grams of a mixture or substance containing methamphetamine, a schedule II controlled substance.

14. On or about October 28, 2019, SPD Detective Calvin Burch obtained a signed search warrant for the DEVICE from the Court of Common Pleas, Clark County, Ohio. The Device was later submitted to the Ohio Narcotic Intelligence Center (ONIC) for an examination consistent with the warrant. On or about January 22, 2020, ONIC generated an Extraction Report from the DEVICE utilizing forensic software.

15. Affiant determined GARZA was previously convicted of an offense punishable by greater than a year in prison, based on a review of court documents. Specifically, GARZA was convicted on or about August 12, 2013, in Montgomery County, Ohio Common Pleas Court, case number 2013 CR 00040/2, of "Aggravated Robbery (deadly weapon)." As such, GARZA is prohibited from possessing firearms and ammunition.

16. Based on my training and experience in investigating firearm and controlled substance violations, I know that individuals routinely utilize their cell phones in furtherance of their criminal activities. Specifically, controlled substance and firearm traffickers often discuss business arrangements via text message, email, social media, and other means of communication. These individuals also often photograph themselves with firearms. These photographs are then stored and maintained on their cell phones.

17. Based on my training and experience; the fact GARZA was in possession of the DEVICE at the time of his arrest in Indiana and had admitted to SPD investigators his ownership of the controlled substances and firearm located at his residence of 1606 Kenwood Avenue, Springfield, Ohio during their interview, and the seizure of controlled substances from his vehicle, I believe that the DEVICE will contain evidence of GARZA's illegal possession of controlled substances in violations of 21 U.S.C. §§ 841(a)(1), (b)(1)(B) and (b)(1)(C) and 18 U.S.C. § 922(g)(1) Possession of a firearm by a Prohibited Person.

18. The DEVICE is currently in the possession of the SPD, located in Springfield, Ohio. In my training and experience, I know that the DEVICE has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state, as they were when the DEVICE first came into the possession of the SPD.

19. Although a forensic extraction from the DEVICE was completed on or about January 22, 2020, there have been multiple updates to the forensic extraction tool, which may have been initially utilized. The updated software may allow for an enhanced extraction of data from the DEVICE. If the updated software version does not support this device, ATF has additional resources to complete an advanced extraction technique on the DEVICE.

20. Based on the foregoing, I respectfully submit that there is probable cause to believe that evidence of a crime - namely, Title 21 U.S.C. §§ 841(a)(1), (b)(1)(B) and (b)(1)(C) – Possession with the Intent to Distribute controlled substances and 18 U.S.C. §§ 922(g)(1)/ 924(a)(2) -Possession of a firearm by a Prohibited Person exists and can be found within the Blue in color, Samsung Galaxy S9+ Smartphone, bearing IMEI number 357930090160505 located in the custody of the Springfield Police Division, Springfield, Ohio.

TECHNICAL TERMS

21. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the

removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

d. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a

keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

e. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP

addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

22. Based on my training, experience, and research, I know that the DEVICE has capabilities that allow it to serve as "a wireless telephone, digital camera, portable media player, GPS navigation device, PDA and Tablet." In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

23. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

24. There is probable cause to believe that things that were once stored on the DEVICE may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been

downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

25. *Forensic evidence.* As further described in Attachment A, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the DEVICE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the DEVICE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual

information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

26. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the DEVICE consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the DEVICE to human inspection in order to determine whether it is evidence described by the warrant.

27. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

28. Based on the above facts and circumstances, I submit that this affidavit supports probable cause for a search warrant authorization the examination of the DEVICE described in attachment A to seek the items described in Attachment B.

Respectfully submitted,

CHRISTOPHER R REED
Digitally signed by CHRISTOPHER REED
Date: 2020.10.23 14:00:34 -04'00'

Christopher Reed
Special Agent, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)

Subscribed and sworn to before me
on October 23, 2020:

Michael J. Newman
United States Magistrate Judge

3:21 PM, Oct 23, 2020

Via electronic means.

ATTACHMENT A

The property to be searched is a Blue Samsung Galaxy S9+ Smartphone, with IMEI number 357930090160505. The DEVICE is currently located in the custody of the Springfield Police Division, Springfield, Ohio. This warrant authorizes the forensic examination of the DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the DEVICE described in Attachment A that relate to violations of 21 U.S.C. §§ 841(a)(1), (b)(1)(B) and (b)(1)(C), and 18 U.S.C. §§ 922(g)(1)/ 924(a)(2) and involve Luis GARZA including:

   a. any communications, including but not limited to: phone calls, text messages, application messages, relating to sources of and possession of controlled substances;

   b. any information related to sources of firearms or controlled substances (including names, addresses, phone numbers, or any other identifying information);

   c. any internet search history and browser files related to sources and possession of controlled substances;

   d. types and amounts of controlled substances possessed as well as dates, places, and amounts of specific transactions;

   e. any information, including GPS location information, recording GARZA's schedule or travel in connection to trafficking in controlled substances;

   f. any photographs and videos, including metadata, and any other records, relating to source or possession of controlled substances; and

g. all bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the ATF may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.